

**DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

SIGNEY STIVENT LÓPEZ RODRIGUEZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA
DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRONICA
VILLAVICENCIO
2020**

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SIGNEY STIVENT LÓPEZ RODRIGUEZ

Diplomado de opción de grado presentado para optar el título de INGENIERO
ELECTRONICO

DIRECTOR:

MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA
DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRONICA
VILLAVICENCIO
2020

NOTA DE ACEPTACIÓN:

Presidente del Jurado

Jurado

Jurado

Villavicencio, 22 de mayo de 2020

AGRADECIMIENTOS

Agradecer primero que todo a DIOS por darme la oportunidad de culminar mi carrera profesional, también a mis padres por haberme brindado su incondicional apoyo para que este gran proyecto se hiciera realidad, además a las otras personas como mis compañeros, e Ingenieros, tutores de cada uno de mis cursos que aportaron su granito de arena para poderme llenar de conocimiento y formarme en este gran camino.

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES	6
LISTA DE TABLAS	7
GLOSARIO.....	8
RESUMEN	9
ABSTRACT	10
INTRODUCCIÓN.....	11
ESCENARIO 1	12
ESCENARIO 2	18
CONCLUSIONES.....	33
BIBLIOGRAFÍA.....	34

LISTA DE ILUSTRACIONES

Ilustración 1. Escenario 1	12
Ilustración 2. Simulación escenario 1	12
Ilustración 3. Tablas de configuración Routers	13
Ilustración 4. Evidencia configuración BGP R1	15
Ilustración 5. Evidencia configuración BGP R2.....	15
Ilustración 6. Evidencia configuración BGP R2 Y R3.....	16
Ilustración 7. Evidencia configuración BGP R3 Y R4.....	17
Ilustración 8. Escenario 2.....	18
Ilustración 9. Simulación escenario 2	18
Ilustración 10. show vtp status SW-AA	20
Ilustración 11. show vtp status SW-BB	20
Ilustración 12. show vtp status SW-CC	21
Ilustración 13. show interfaces SW-AA	22
Ilustración 14. show interfaces SW-BB	22
Ilustración 15. show interfaces trunk SW-AA	23
Ilustración 16. Show vlan brief SW-AA.....	25
Ilustración 17. Show vlan brief SW-AA.....	25
Ilustración 18. Configuraciones PCs Switch SW-AA.....	28
Ilustración 19. Configuraciones PCs Switch SW-BB.....	28
Ilustración 20. Configuraciones PCs Switch SW-CC.....	29
Ilustración 21. Prueba ping Pcs.....	31

LISTA DE TABLAS

Tabla 1. Configuraciones a asignar Interfaz, VLAN e IP	26
Tabla 2. Configuraciones, Switch, Interfaz, Ip y máscara.....	29
Tabla 3. Datos para pruebas de ping	30

GLOSARIO

CCNP: (*Cisco Certified Network Professional*) es el nivel intermedio de certificación de la compañía. Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos.

PROTOCOLOS DE RED: Conjunto de normas estándares que especifican el método para el envío y recibimiento de datos entre varios ordenadores. También conocida como una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

BGP: Protocolo de puerta de enlace de frontera, permite el intercambio de información entre grandes nodos de Internet encontrando el camino más eficiente para transferir una gran cantidad de información entre dos puntos de red.

DHCP: Protocolo de configuración dinámica de host, es de tipo cliente/servidor mediante el cual un servidor de red DHCP asigna de forma dinámica las direcciones IP y otros parámetros de configuración de red a los diferentes dispositivos conectados.

OSPF: Protocolo que consiste en realizar una comunicación mediante La ruta más corta y obtener beneficios para la comunicación

NETWORKING: Es una red de ordenadores o también conocida como red de comunicaciones de datos, reconectados entre sí por medio de dispositivos físicos, que se encarga en el envío y recibimiento impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios para los usuarios.

GNS3: Simulador gráfico de red lanzado en 2008, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

ROUTER: Dispositivo que proporciona conectividad a nivel de red. Se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red.

RESUMEN

En este documento encontraremos información del desarrollo de la prueba de habilidades del módulo de cisco CCNP, en esta se plantea la solución de dos escenarios, en el primero se debe realizar la configuración en una relación de vecino BGP entre cuatro Routers, en el segundo escenario debemos realizar la configuración de tres switch que deberán usar VTP para obtener las actualizaciones VLAN también se realizara configuración DTP (Dynamic Trunking Protocol) y por último la asignación de Ip.

Es inevitable señalar que el diplomado de CCNP es muy importante e indispensable para la personas que requieran adquirir el conocimiento necesario para configurar, instalar, y manejar redes de todo tipo, apoyados en los distintos protocolos y tecnologías actuales como EIGRP, BGP, TCP/IP, OSPF, ISDN, Frame Relay, STP y VTP, Route Avanzado, y Switch Avanzado, se explican con detalle cada uno de los comandos y sus respectivas funciones del proceso, haciendo de una forma más practica la adquisición de estos conocimientos.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this document we will find information on the development of the skills test of the Cisco CCNP module, in this the solution of two scenarios is proposed, in the first one the configuration must be done in a BGP neighbor relationship between four Routers, in the second scenario We must make the configuration of three switches that must use VTP to obtain the VLAN updates. DTP (Dynamic Trunking Protocol) configuration will also be made and finally the allocation of Ip.

It is important to note that the CCNP diploma is very important and indispensable for people who require to acquire the knowledge of how to configure, install, and manage networks of all kinds, supported by the different protocols and current technologies such as EIGRP, BGP, TCP / IP , OSPF, ISDN, Frame Relay, STP and VTP, Route Advanced, and Switch Advanced, each of the commands and their respective process functions are explained in detail, making the acquisition of this knowledge more practical.

Key Words: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCIÓN

El presente documento se realizó con el objetivo principal de dejar evidencia de la sustentación de evaluación de la prueba de habilidades prácticas del diplomado CCNP, en este encontramos la solución a los dos escenarios propuestos con sus respectivos pasos requeridos para el desarrollo de estos, así como también se evidencian las diferentes líneas de comandos utilizados. Se implementaron los diferentes protocolos de comunicación que se fueron aprendiendo en el progreso del diplomado de CISCO los cuales fueron indispensables para practicar las diferentes habilidades adquiridas y así poder llegar a la solución de los escenarios propuestos.

En los escenarios propuestos se debe realizar la configuración de dos tipos de dispositivos diferentes como lo son Switchs y Routers. Estos dispositivos son de gran importancia a la hora que se requieren manejar grandes volúmenes de información en las distintas redes de trabajo ya que cada vez se hace más complejo debido a la necesidad de mantener un servicio constante que brinde la conectividad y disponibilidad suficiente de los datos a los usuarios cuando estos lo requieran.

Por otra parte, es importante señalar que el protocolo BGP es de tipo exterior, tipo path Vector y no Hierarchy Required y se usa para sistemas autónomos en el escenario uno cuando se realiza la configuración vecino que se señala es para permitir la comunicación entre el routers y sus Loopbacks.

En el escenario dos los switch están en configuración de modo troncal permiten la comunicación entre ellos, y así logran llegar a diferentes dispositivos conectados a estos y que se direccionaron por sus interfaces a las Vlans; para esto también se requiere el soporte de la configuración VTP (Vlan Trunking Protocol), que nos admitirá hacer la configuración y administración de Vlans.

ESCENARIO 1

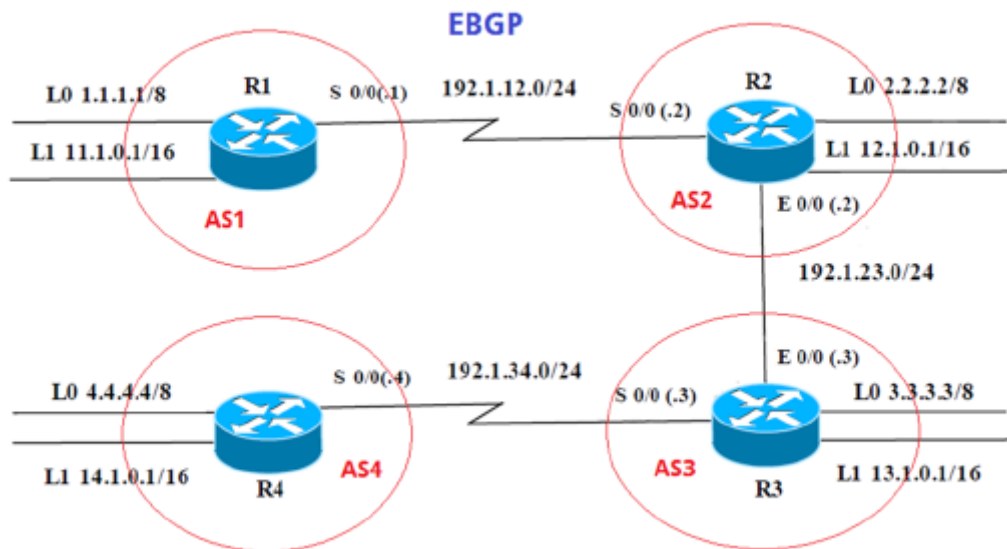


Ilustración 1. Escenario 1

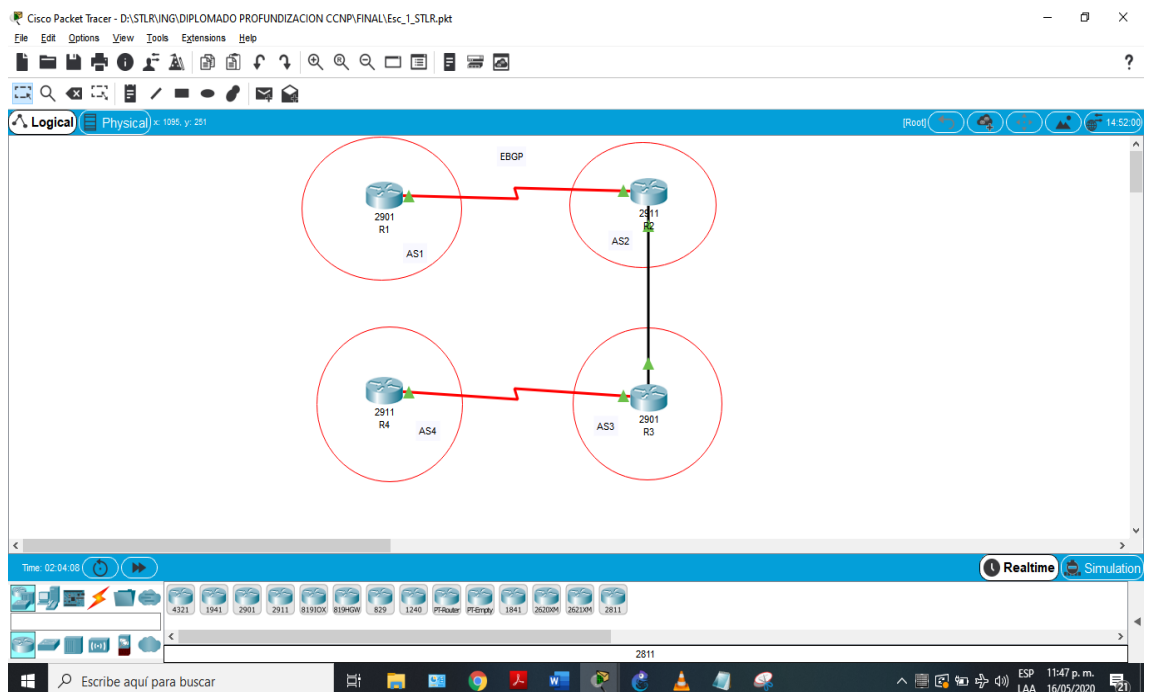


Ilustración 2. Simulación escenario 1

Información para la configuración de los Routers

R1	Interfaz	Dirección IP	Máscara
	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/0	192.1.12.1	255.255.255.0

R2	Interfaz	Dirección IP	Máscara
	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0

R3	Interfaz	Dirección IP	Máscara
	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 0/0	192.1.23.3	255.255.255.0
	S 0/0	192.1.34.3	255.255.255.0

R4	Interfaz	Dirección IP	Máscara
	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 0/0	192.1.34.4	255.255.255.0

Ilustración 3. Tablas de configuración Routers

1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en **AS1** y R2 debe estar en **AS2**. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

Comandos utilizados configuración BGP, asignación de Loopback e ID

R1

```

interface Loopback0
ip address 1.1.1.1 255.0.0.0

interface Loopback1
ip address 11.1.0.1 255.255.0.0

interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
    
```

shutdown

```
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
```

```
interface Serial0/0/0
ip address 192.1.12.1 255.255.255.0
```

```
router bgp 1
bgp router-id 22.22.22.22
bgp log-neighbor-changes
no synchronization
neighbor 192.1.12.2 remote-as 2
network 1.0.0.0
network 11.1.0.0 mask 255.255.0.0
```

R2

```
interface Loopback0
ip address 2.2.2.2 255.0.0.0
interface Loopback1
ip address 12.1.0.1 255.255.0.0
```

```
interface GigabitEthernet0/0
ip address 192.1.23.2 255.255.255.0
duplex auto
speed auto
```

```
router bgp 2
bgp router-id 33.33.33.33
bgp log-neighbor-changes
no synchronization
neighbor 192.1.12.1 remote-as 1
network 2.0.0.0
network 12.1.0.0 mask 255.255.0.0
```

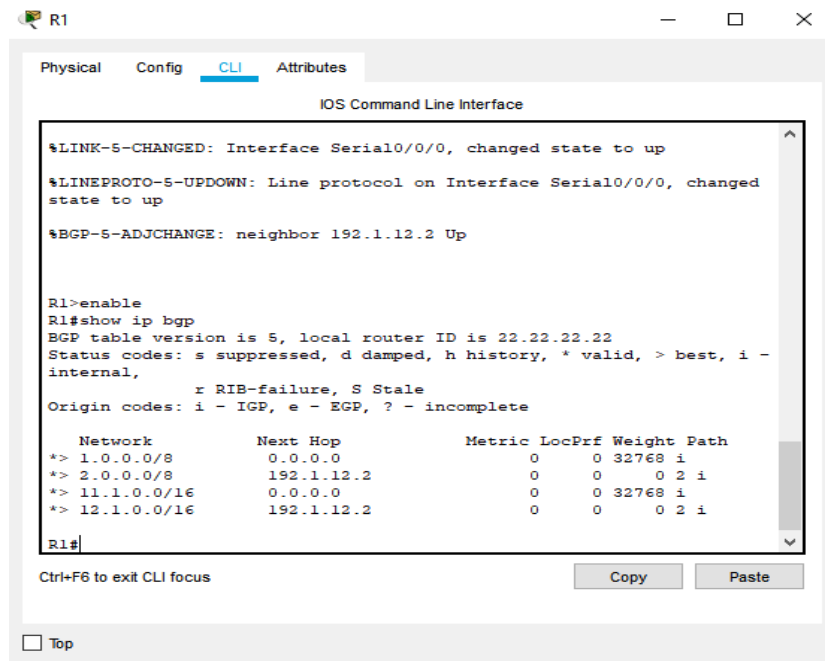


Ilustración 4. Evidencia configuración BGP R1

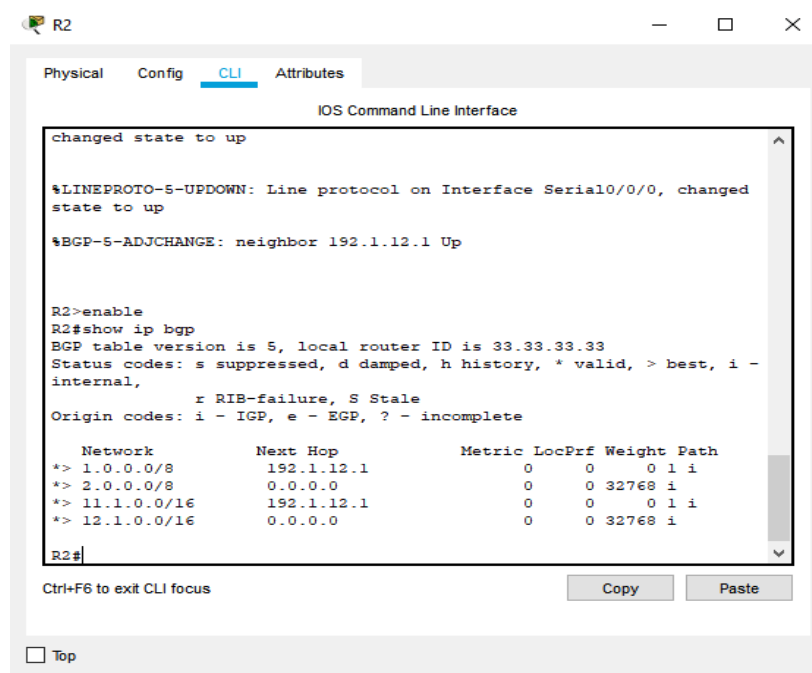


Ilustración 5. Evidencia configuración BGP R2

- Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en **AS2** y R3 debería estar en **AS3**. Anuncie las

direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

Commandos utilizados

```
router bgp 3
bgp router-id 44.44.44.44
bgp log-neighbor-changes
no synchronization
neighbor 192.1.23.2 remote-as 2
network 3.0.0.0
network 13.1.0.0 mask 255.255.0.0
```

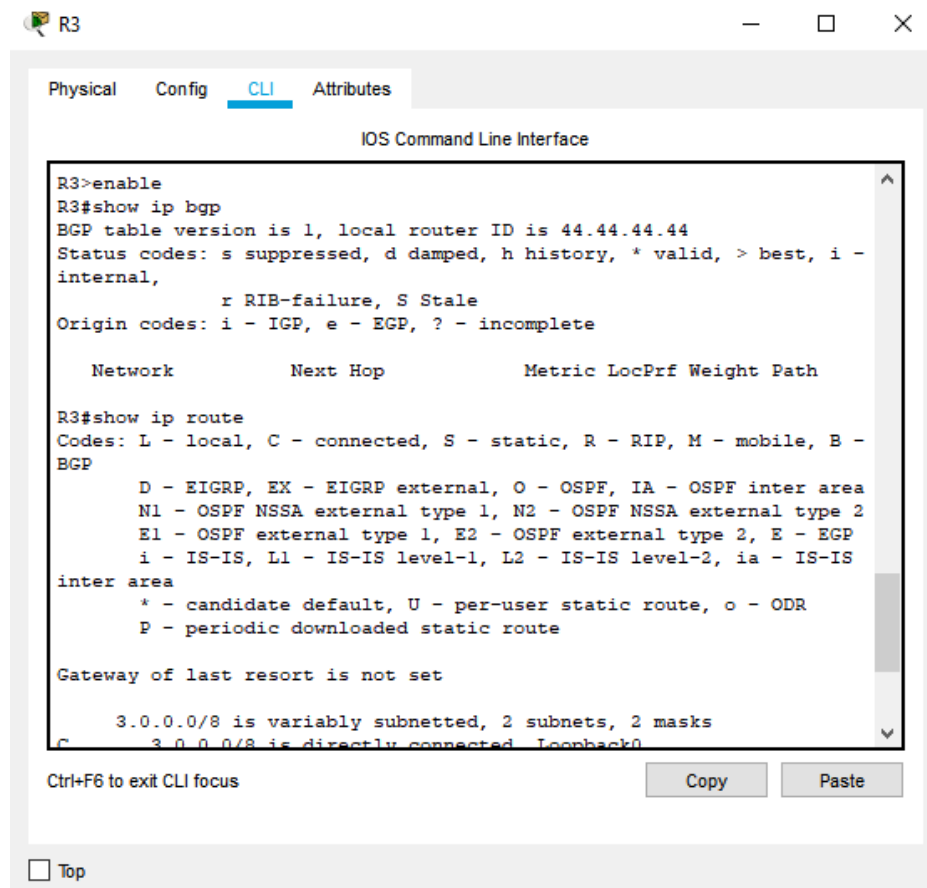


Ilustración 6. Evidencia configuración BGP R2 Y R3

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4

como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

Comandos utilizados

```
interface Loopback0
```

```
ip address 4.4.4.4 255.0.0.0
```

```
interface Loopback1
```

```
ip address 14.1.0.1 255.255.0.0
```

```
interface Serial0/0/0
```

```
ip address 192.1.34.4 255.255.255.0
```

```
router bgp 4
```

```
bgp router-id 66.66.66.66
```

```
bgp log-neighbor-changes
```

```
no synchronization
```

```
neighbor 192.1.34.3 remote-as 3
```

```
network 4.0.0.0
```

```
network 14.1.0.0 mask 255.255.0.0
```

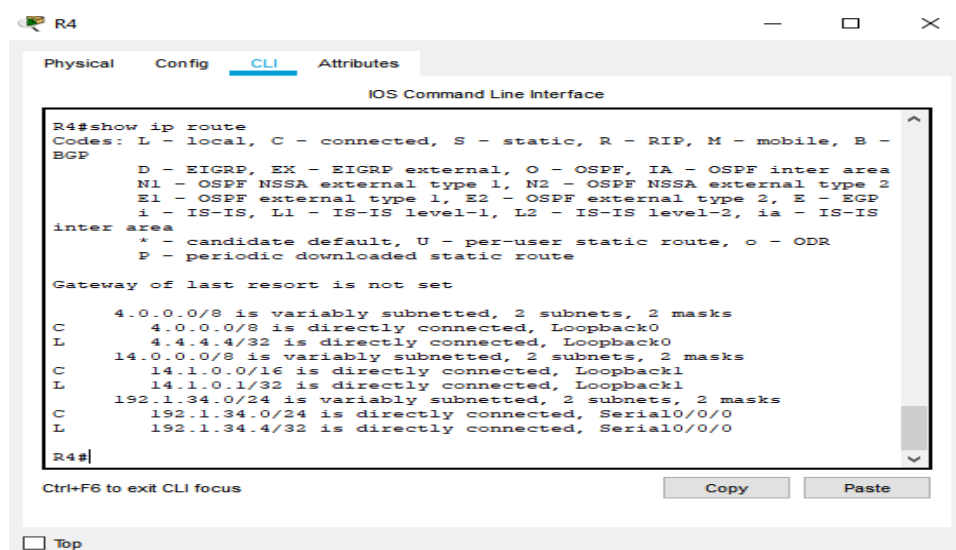


Ilustración 7. Evidencia configuración BGP R3 Y R4

ESCENARIO 2

Topología de red

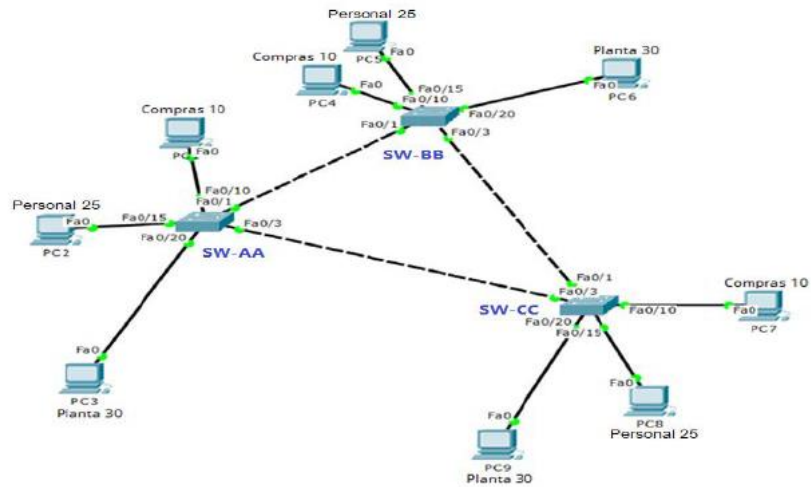


Ilustración 8. Escenario 2

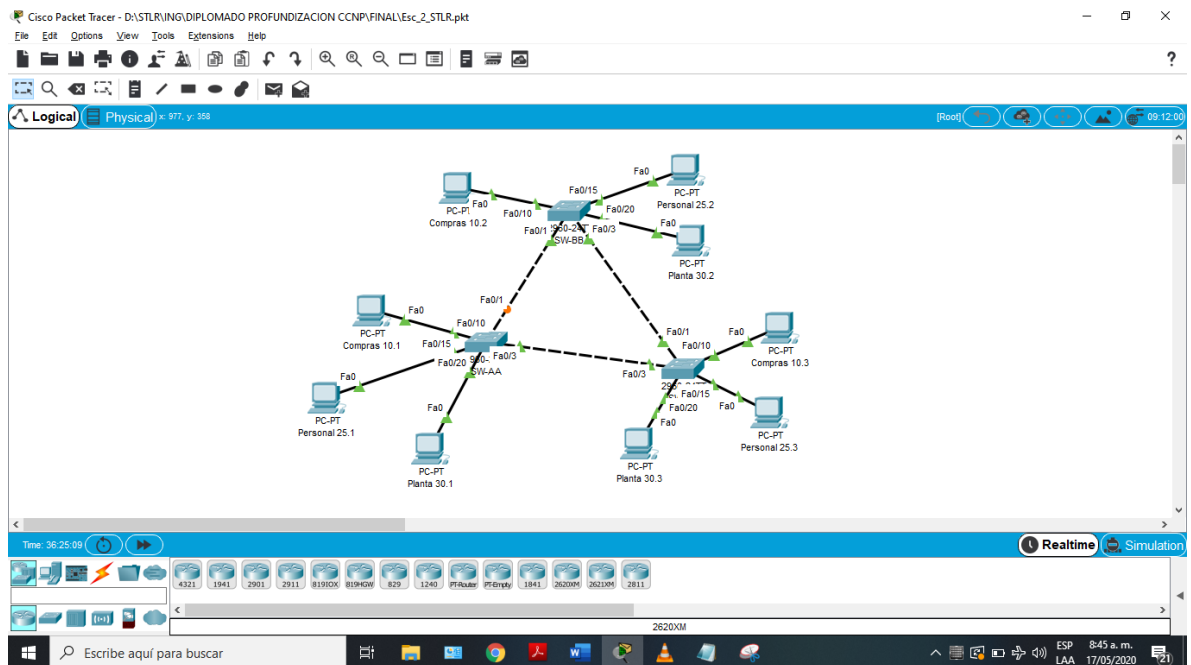


Ilustración 9. Simulación escenario 2

A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

Comandos utilizados configuración VTP

VTP SW-BB

```
hostname SW-BB  
VTP domain CCNP  
VTP pass cisco  
VTP mode server
```

VTP SW-AA

```
hostname SW-AA  
VTP domain CCNP  
VTP pass cisco  
VTP mode client
```

VTP SW-CC

```
hostname SW-CC  
VTP domain CCNP  
VTP pass cisco  
VTP mode client
```

2. Verifique las configuraciones mediante el comando show vtp status.

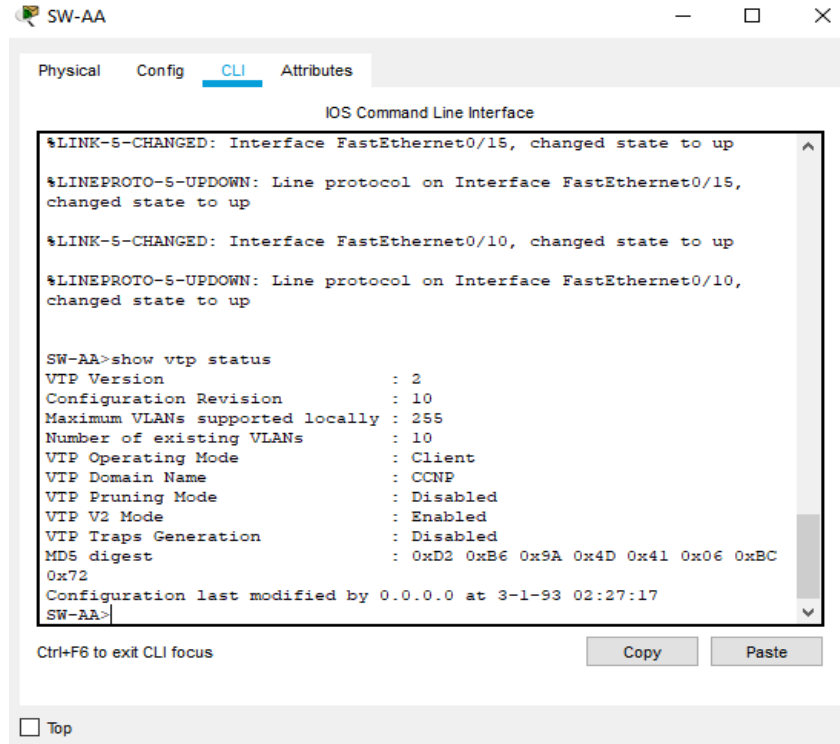


Ilustración 10. show vtp status SW-AA

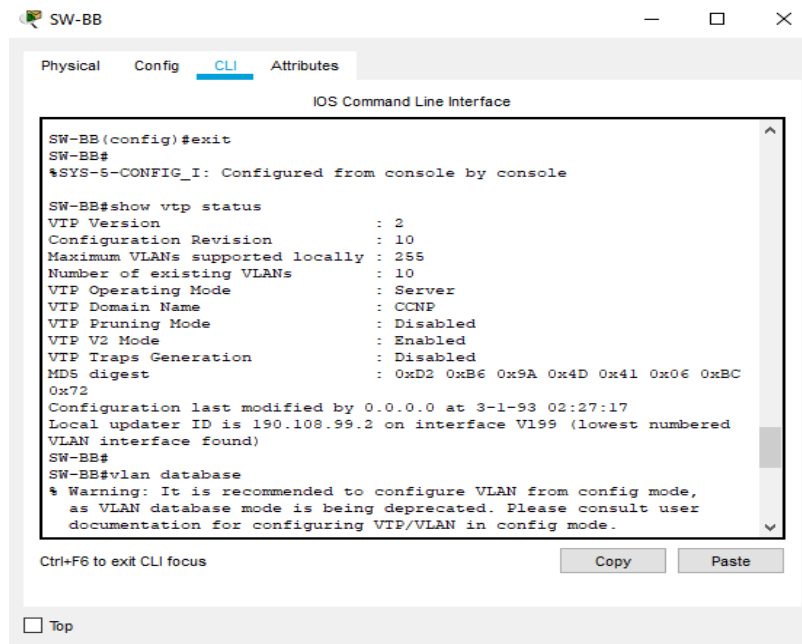


Ilustración 11. show vtp status SW-BB

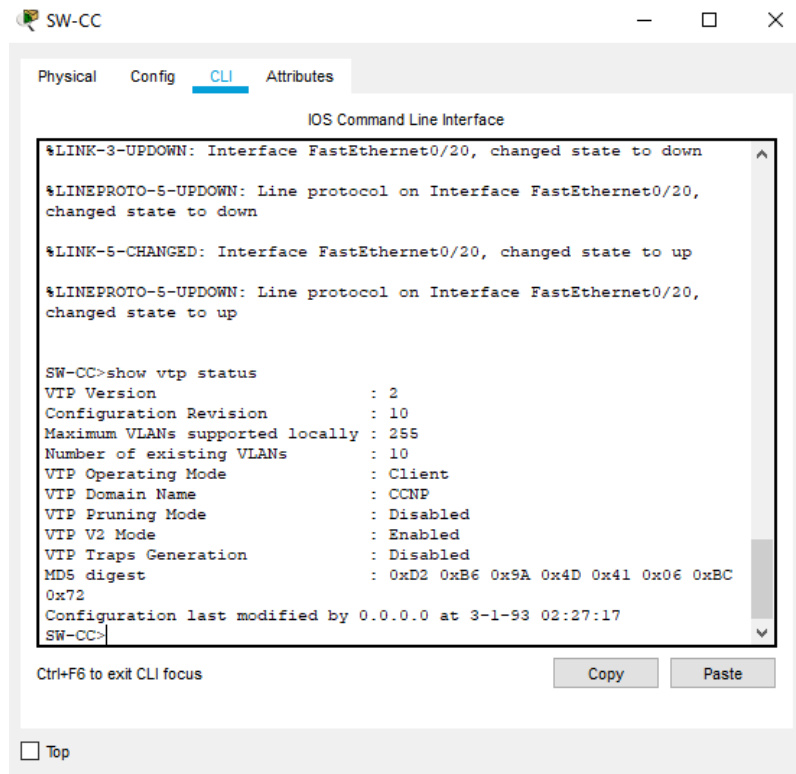


Ilustración 12. show vtp status SW-CC

B. Configurar DTP (Dynamic Trunking Protocol)

4. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

Comando utilizado para configuración

int f0/1

switchport mode Dynamic desirable

5. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando **show interfaces trunk**.

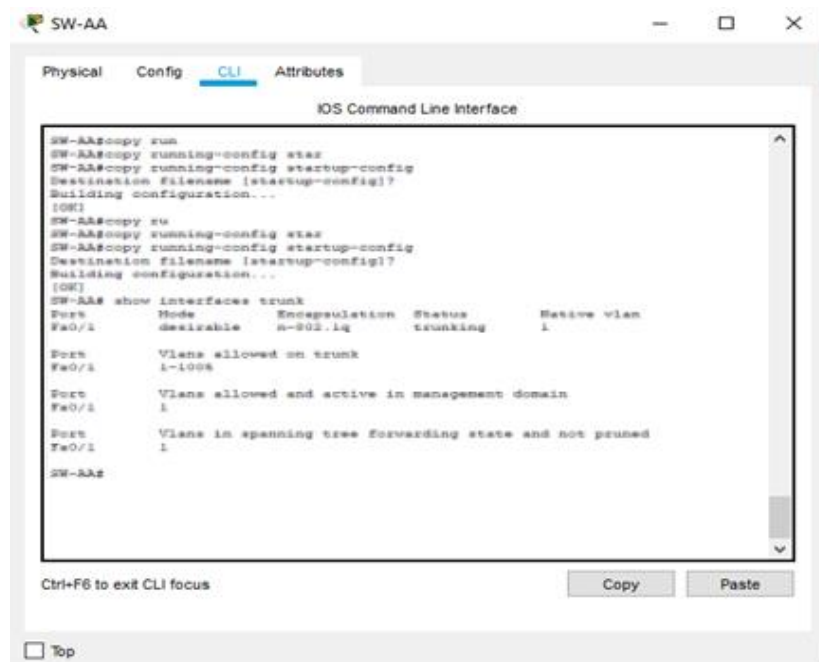


Ilustración 13. show interfaces SW-AA

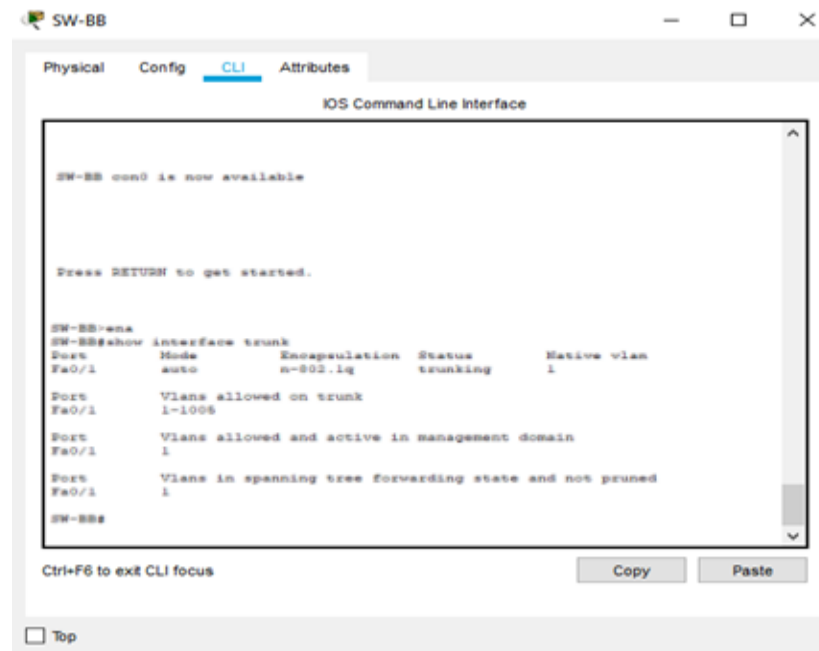
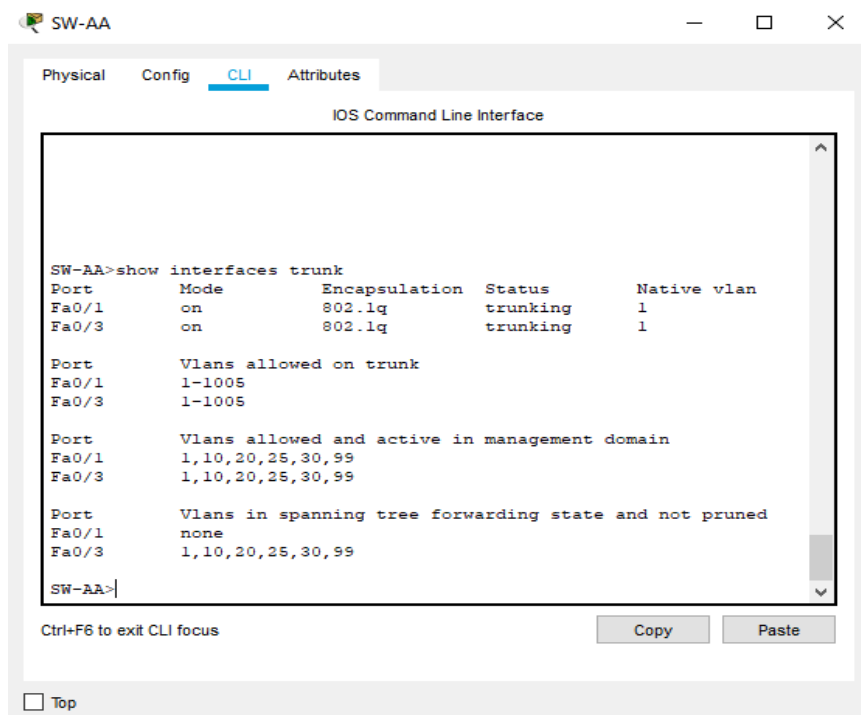


Ilustración 14. show interfaces SW-BB

6. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SW-AA

7. Verifique el enlace "trunk" el comando show interfaces trunk en SW-AA.



The screenshot shows a window titled 'SW-AA' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The command 'SW-AA>show interfaces trunk' has been entered, and the output is displayed in a table format. The output shows that both Fa0/1 and Fa0/3 are configured as trunk ports with 802.1q encapsulation and native VLAN 1. It also lists the VLANs allowed on the trunk (1-1005) and the VLANs allowed and active in the management domain (1, 10, 20, 25, 30, 99). Finally, it shows the VLANs in the spanning tree forwarding state and not pruned, which are the same as the active VLANs.

```
SW-AA>show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Fa0/1     on        802.1q         trunking      1
Fa0/3     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,25,30,99
Fa0/3     1,10,20,25,30,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none
Fa0/3     1,10,20,25,30,99

SW-AA>
```

Ilustración 15. show interfaces trunk SW-AA

8. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

Comandos utilizados para el enlace "trunk"

SW-BB
Int f0/3
Switchport mode trunk

C. Agregar VLANs y asignar puertos.

9. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANs Compras (10), Personal (25), Planta (30) y Admon (99)

En SW-AA no es posible agregar VLAN 10 debido a la configuración VTP VLAN que posee, asimismo también cuenta con el modo cliente. Es predecible decir que basta con la configuración de SW-BB ya que estando configurado este, deben aparecer las VLAN en el switch SW-AA.

Comandos de configuración SW-BB

Vlan 10
Name compras
Vlan 25
Name personal
Vlan 30
Name planta
Vlan 99
Name admon

10. Verifique que las VLANs han sido agregadas correctamente.

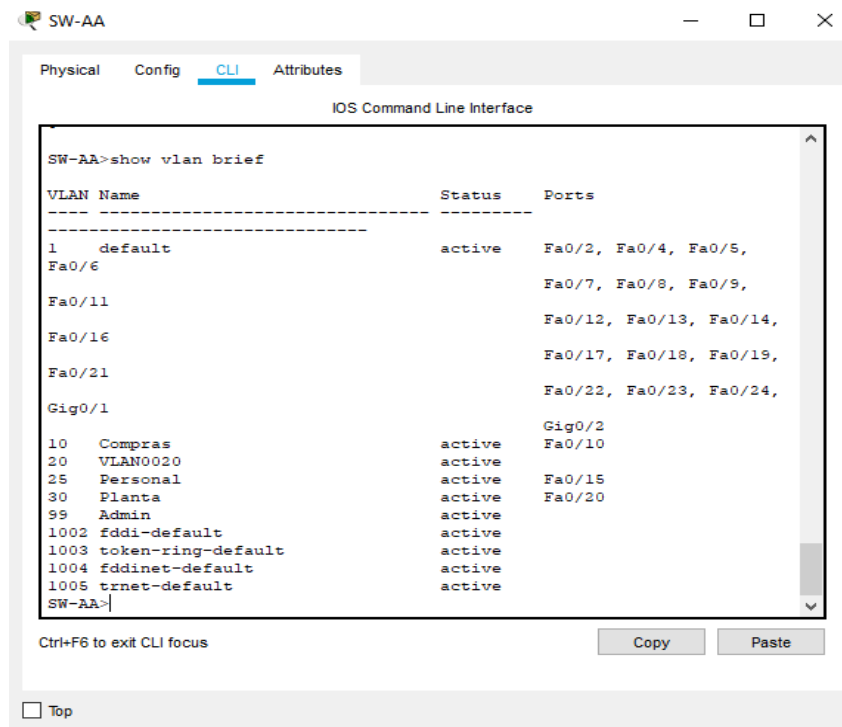


Ilustración 16. Show vlan brief SW-AA

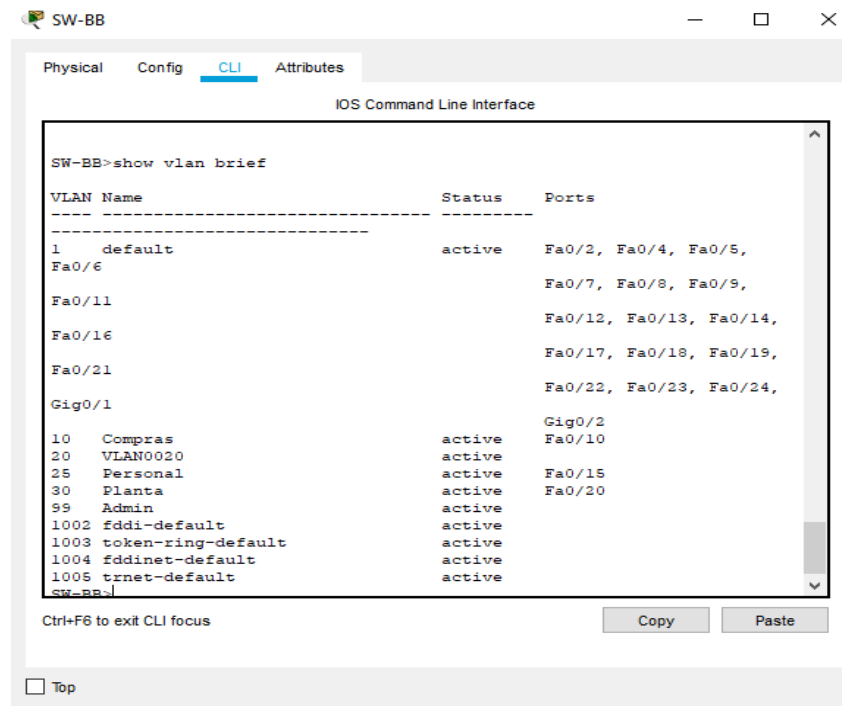


Ilustración 17. Show vlan brief SW-AA

11. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X / 24
F0/20	VLAN 30	190.108.30.X / 24

X = número de cada PC particular

Tabla 1. Configuraciones a asignar Interfaz, VLAN e IP

12. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

Comandos utilizados para realizar las configuraciones

SW-AA

```
Int f0/10
Switchport mode Access
Switchport Access vlan 10
No shutdown
Exit
```

SW-BB

```
Int f0/10
Switchport mode Access
Switchport Access vlan 10
No shutdown
Exit
```

SW-CC

```
Int f0/10
Switchport mode Access
Switchport Access vlan 10
No shutdown
Exit
```

13. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

Comandos utilizados para realizar las configuraciones

SW-AA

```
Int f0/15
Switchport mode access
Switchport access vlan 25
No shutdown
Exit
```

```
Int f0/20
Switchport mode access
Switchport access vlan 30
No shutdown
Exit
```

SW-BB

```
Int f0/15
Switchport mode access
Switchport access vlan 25
No shutdown
Exit
```

```
Int f0/20
Switchport mode access
Switchport access vlan 30
No shutdown
Exit
```

SW-CC

```
Int f0/15
Switchport mode access
Switchport access vlan 25
No shutdown
Exit
```

```
Int f0/20
Switchport mode access
Switchport access vlan 30
```

No shutdown

Exit

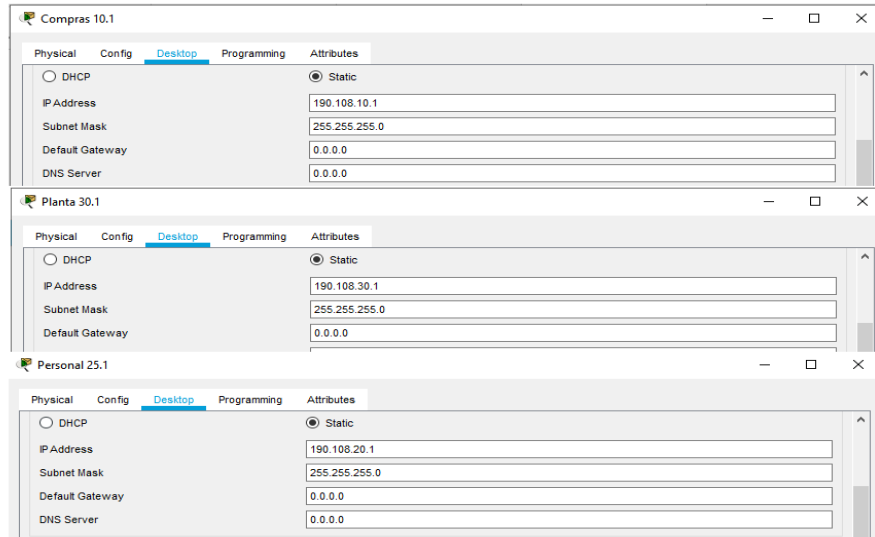


Ilustración 18. Configuraciones PCs Switch SW-AA

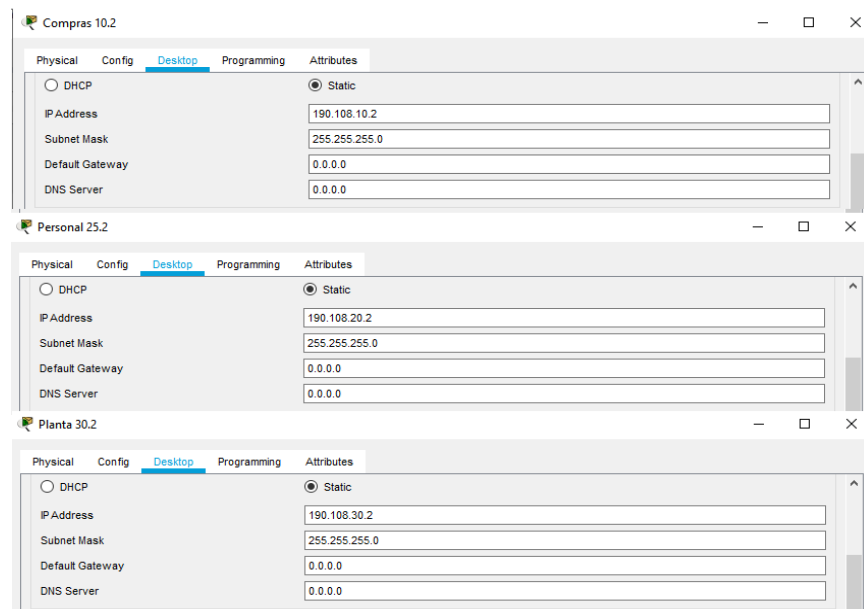


Ilustración 19. Configuraciones PCs Switch SW-BB

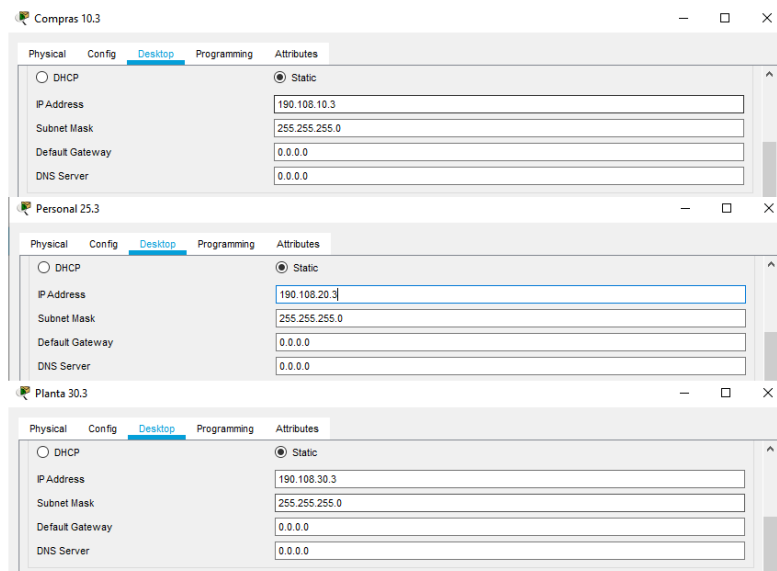


Ilustración 20. Configuraciones PCs Switch SW-CC

D. Configurar las direcciones IP en los Switches.

14. En cada uno de los Switches asigne una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

Tabla 2. Configuraciones, Switch, Interfaz, Ip y máscara.

Comandos utilizados para realizar las configuraciones

SW- AA
Vlan 99
Exit

```

Interface vlan 99
Ip address 190.108.99.1 255.255.255.0
No shutdown
Exit
Ip routing

```

SW – BB

```

Vlan 99
Exit
Interface vlan 99
Ip address 190.108.99.2 255.255.255.0
No shutdown
Exit
Ip routing

```

SW – CC

```

Vlan 99
Exit
Interface vlan 99
Ip address 190.108.99.3 255.255.255.0
No shutdown
Exit
Ip routing

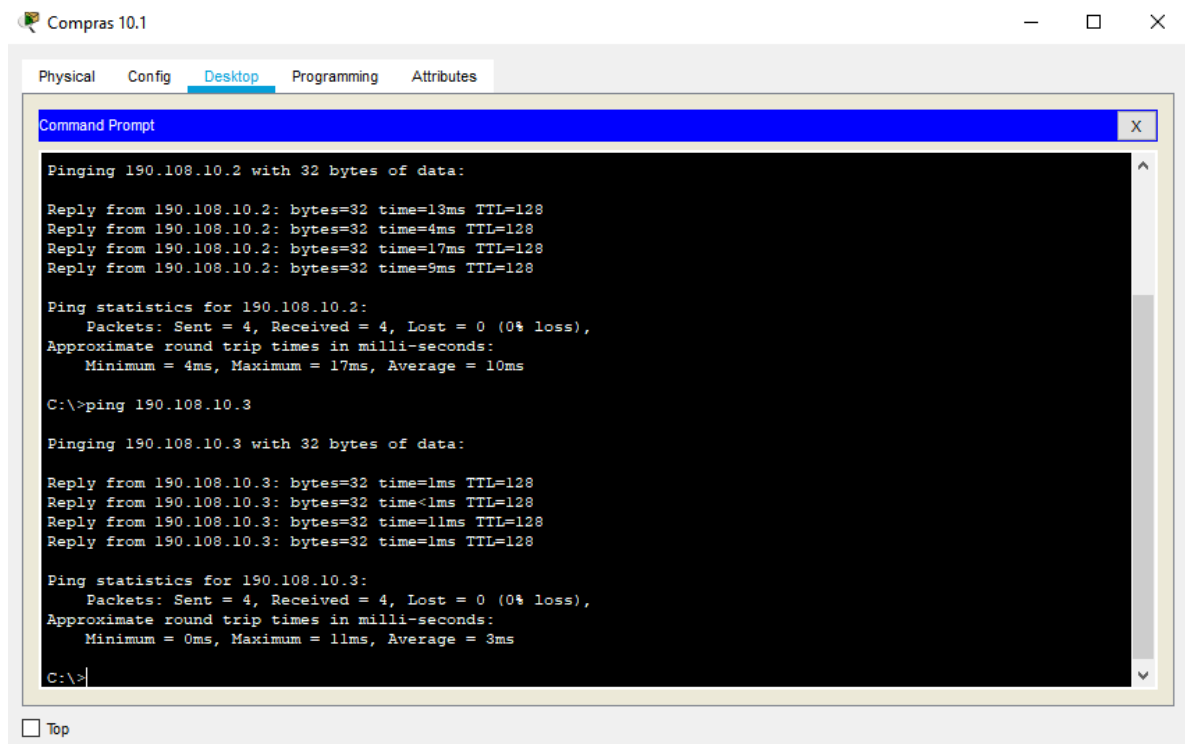
```

E. Verificar la conectividad Extremo a Extremo

15. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

SWITCH	PCs		
	COMPRAS	PERSONAL	PLANTA
SW-AA	190.108.10.1	190.108.20.1	190.108.30.1
SW-BB	190.108.10.2	190.108.20.2	190.108.30.1
SW-CC	190.108.10.3	190.108.20.3	190.108.30.1

Tabla 3. Datos para pruebas de ping



The screenshot shows a Cisco Packet Tracer window titled 'Compras 10.1'. It has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The 'Desktop' tab is active, displaying a 'Command Prompt' window. The Command Prompt shows the results of two ping commands. The first command is 'ping 190.108.10.2', which shows four successful replies with varying round trip times (13ms, 4ms, 17ms, 9ms) and a TTL of 128. The statistics show 4 packets sent, 4 received, and 0% loss. The second command is 'ping 190.108.10.3', which also shows four successful replies with round trip times of 1ms, 1ms, 11ms, and 1ms, and a TTL of 128. The statistics show 4 packets sent, 4 received, and 0% loss. The Command Prompt window has a 'Top' button at the bottom left.

```
Pinging 190.108.10.2 with 32 bytes of data:

Reply from 190.108.10.2: bytes=32 time=13ms TTL=128
Reply from 190.108.10.2: bytes=32 time=4ms TTL=128
Reply from 190.108.10.2: bytes=32 time=17ms TTL=128
Reply from 190.108.10.2: bytes=32 time=9ms TTL=128

Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 17ms, Average = 10ms

C:\>ping 190.108.10.3

Pinging 190.108.10.3 with 32 bytes of data:

Reply from 190.108.10.3: bytes=32 time=1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time=11ms TTL=128
Reply from 190.108.10.3: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>
```

Ilustración 21. Prueba ping Pcs

Se evidencia un ping exitoso sin pérdida de paquetes debido a que los PCs tienen la misma VLAN y se encuentran en la misma red, por otra parte, cabe aclarar que los que tienen la VLAN diferente el ping es fallido. La comunicación para los switches se establece por truncamiento y para los Pcs por intermedio de las VLANs. Gracias a esto se logra comunicar un Pc con la misma VLAN y red que se localiza conectado en otro switch.

16. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.

El ping que obtenemos al ejecutarlo a cada uno de los Switch es exitoso, esto gracias a que se ejecutó una comunicación por truncamiento en ellos. También al establecer la interface virtual del switch a cada uno de ellos se le realizó la misma configuración de la VLAN, y en la misma red.

17. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito

En este caso cuando ejecutamos el ping detectamos que no tiene éxito, aun existiendo la comunicación por truncamiento entre los switchs, los Pcs y sus interfaces de conexión con los switch se configuraron en una VLAN distinta a la VLAN que tienen configurado los switch (SVI). Por otra también encontramos que los Pcs y los switchs se encuentran en redes diferentes.

CONCLUSIONES

Puedo decir que una vez más se logra con idoneidad la correcta configuración y administración de dispositivos de Networking, en diseños de redes de conmutación o escalables, esto gracias a los conocimientos desarrollados durante el progreso del diplomado de profundización de CCNP, y así establecer niveles de seguridad básicos en una red general.

Entendimos que con la creación de áreas de enrutamiento se reduce cuantiosamente el número de rutas que se propagan y se mejora la posibilidad de redistribuir redes en cada uno de los diferentes protocolos

Es importante destacar todo lo que podemos lograr gracias a las herramientas de simulación como lo son Packet Tracer, GNS3, SMARTLAB ya que nos permite practicar con cualquier ejercicio que se nos pueda presentar en los diferentes entornos de la vida real para así ir obteniendo el conocimiento necesario de cada uno de los distintos protocolos, dispositivos, comandos e instrucciones que se deben utilizar para tener un procedimiento adecuado y comprender más a fondo las características de cada una de las redes que se encuentra.

BIBLIOGRAFÍA

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de: <https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1lInWR0hoMxgBNv1CJ>

Macfarlane, J. (2014). Network Routing Basics: Understanding IP Routing in Cisco Systems. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de: <https://1drv.ms/b/s!AmlJYei-NT1lInMfy2rhPZHwEoWx>